IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Applicant:	Franck Le
Title:	IPV6 ADDRESS OWNERSHIP SOLUTION BASED ON ZERO-KNOWLEDGE IDENTIFICATION PROTOCOLS OR BASED ON ONE TIME PASSWORD
Appl. No.:	10/615,829
Filing Date:	7/10/2003
Examiner:	Yogesh Paliwal
Art Unit:	2435
Confirmation Number:	8920

BRIEF ON APPEAL

Mail Stop Appeal Brief - Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir/Madam:

This Appeal Brief is being filed in response to an Advisory Action dated October 20, 2008, maintaining the rejection of Claims 29-47 and indicating that the Amendment and Reply under 37 C.F.R. § 1.116 dated September 25, 2008, in response to the Final Office Action dated August 1, 2008, would not be entered. A Notice of Appeal was mailed on December 2, 2008, making February 2, 2009, two-months from the date of filing the Notice of Appeal. As a result, the submission of this Appeal Brief under the provisions of 37 C.F.R. § 41.37 is timely filed. This Appeal Brief is being filed together with a credit card payment in the amount of $540.00 covering the 37 C.F.R. 41.20(b)(2) appeal fee. If this fee is deemed to be insufficient, authorization is hereby given to charge any deficiency (or credit any balance) to the undersigned deposit account 19-0741.

Appellant respectfully requests reconsideration of the Application.

REAL PARTY IN INTEREST

The real party in interest is Spyder Navigations L.L.C., the assignee of record, having a place of business at 1209 Orange Street, Wilmington, Delaware 19801 USA. The assignment to Spyder Navigations L.L.C. was recorded in the records of the United States Patent and Trademark Office at Reel/Frame 019659/0074 on August 7, 2007.

RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences that will directly affect, be directly affected by, or have a bearing on the present appeal, that are known to Appellants or Appellant's patent representative.

STATUS OF CLAIMS

Claims 1-28 and 48-89 have been cancelled. The present appeal is directed to Claims 29-47, all of which stand rejected pursuant to a Final Office Action dated August 1, 2008, and an Advisory Action dated October 20, 2008. Claims 29-47 are being appealed. Claims 1-89 with the appropriate status reference are shown in the attached Claims Appendix.

STATUS OF AMENDMENTS

A Final Office Action dated August 1, 2008 was received by Appellant. In an Amendment and Reply under 37 C.F.R. § 1.116 dated September 25, 2008, Claims 29, 31, 36, 38, 42, and 44 were amended, and Claims 33, 34, 40, and 46 were canceled. The elements of canceled Claims 33, 34, 40, and 46 were incorporated into Claims 29, 36, and 42. Claims 31, 38, and 44 were amended based on the amendment to Claims 29, 36, and 42, (hereinafter, "the Final Office Action Amendments").

As a result of these amendments, Claims 29-32, 35-39, 41-45, and 47 were pending in the Application when an Advisory Action dated October 20, 2008, was issued by the Examiner. In the Advisory Action, the Examiner refused to enter the Final Office Action Amendments.

Appellant submits that the Amendment and Reply under 37 C.F.R. § 1.116 dated September 25, 2008, including the Final Office Action Amendments should have been entered because the amendment incorporated features into independent Claims 29, 36, and 42 that were previously presented in Claims 33, 34, 40, and 46. As such, the Examiner had already examined these claims, and therefore, no new search or consideration was required. On the continuation sheet of the Advisory Action dated October 20, 2008, the Examiner stated that the amendments change "the scope of dependent claims 30, 32, 35, 37-39, 41, 43-45 and 47 (these claims were never examined with the proposed scope)." Appellant disagrees and respectfully submits that the amendments merely included features from dependent claims into the independent claims to place the claims in better form for appeal. As a result, the Amendment and Reply under 37 C.F.R. § 1.116 dated September 25, 2008, the Final Office Action Amendments, should have been entered.

Thus, because the the Final Office Action Amendments were not entered, no amendments have been made in the present Application subsequent to receipt of the Final Office Action dated August 1, 2008.

SUMMARY OF CLAIMED SUBJECT MATTER

Three independent claims, Claims 29, 36, and 42, are under appeal and argued below. Additionally, dependent claims 31-34, 38-40, and 44-46 are separately argued.

Claim 29 is directed to a method for confirming ownership of an address by a first device to a second device. (e.g. paras. [0156]-[0165], pg. 7, lines 21-2). A number of

identifications allowed is identified. (e.g. para. [0158], pg. 7, lines 33-35). A secret value is identified at a first device, wherein the number of identifications allowed is based on a maximum number of times the secret value may be used before the secret value is changed. (e.g. paras. [0157]-[0158], pg. 7, lines 27-35). A first address value is calculated based on the identified secret value and the identified number of identifications allowed. (e.g. para. [0159], pg. 7, lines 36-42). An address is generated as a concatenation of a second address value and the calculated first address value. (e.g. para. [0159], pg. 7, lines 36-42). The generated address is sent from the first device to a second device. (e.g. para. [0051], pg. 3, lines 7-10; para. [0068], pg. 4, lines 11-14). A request to confirm ownership of the generated address is received from the second device at the first device. (e.g. para. [0069], pg. 4, lines 24-25). A number of confirmations previously performed between the first device and the second device is identified. (e.g. para. [0162], pg. 7, lines 43-47). A first value is calculated based on the identified secret value and the identified number of confirmations performed. (e.g. paras. [0162]-[0164], pg. 7, lines 43-53). A first message including the calculated first value is sent from the first device to the second device to confirm ownership of the generated address by the first device. (e.g. paras. [0162]-[0164], pg. 7, lines 43-53).

Claim 31 depends from Claim 29 and further comprises repeating the receiving of the request to confirm ownership, the identification of the number of confirmations previously performed between the first device and the second device, the calculation of the first value, and the sending of the first message including the calculated first value. (e.g. para. [0162], pg. 7, lines 43-47).

Claim 32 depends from Claim 31 and further recites that the first message further includes the identified number of confirmations performed. (e.g. para. [0162], pg. 7, line 47).

Claim 33 depends from Claim 29 and further comprises comparing the identified number of confirmations performed with the identified number of identifications allowed, and based on an outcome of the comparison, identifying a second secret value at the first device. (e.g. para. [0158], pg. 7, lines 33-35).

Claim 34 depends from Claim 33 and further comprises repeating the calculation of the first address value, the generation of the address, the sending of the generated address, the receiving of the request to confirm ownership, the identification of the number of confirmations previously performed between the first device and the second device, the calculation of the first value, and the sending of the first message including the calculated first value. (e.g. para. [0158], pg. 7, lines 33-35).

Claim 36 is directed to a communication device including a processor, a communication interface operably coupled to the processor, and a computer-readable medium including computer-readable instructions stored therein. Upon execution by the processor, the computer-readable instructions cause the communication device to perform the operations of Claim 29. A number of identifications allowed is identified. (e.g. para. [0158], pg. 7, lines 33-35). A secret value is identified at a first device, wherein the number of identifications allowed is based on a maximum number of times the secret value may be used before the secret value is changed. (e.g. paras. [0157]-[0158], pg. 7, lines 27-35). A first address value is calculated based on the identified secret value and the identified number of identifications allowed. (e.g. para. [0159], pg. 7, lines 36-42). An address is generated as a concatenation of a second address value and the calculated first address value. (e.g. para. [0159], pg. 7, lines 36-42). The generated address is sent from the first device to a second device. (e.g. para. [0051], pg. 3, lines 7-10; para. [0068], pg. 4, lines 11-14). A request to confirm ownership of the generated address is received from the second device at the first device. (e.g. para. [0069], pg. 4, lines 24-25). A number of confirmations previously performed between the first device and the second device is identified. (e.g.

para. [0162], pg. 7, lines 43-47). A first value is calculated based on the identified secret value and the identified number of confirmations performed. (e.g. paras. [0162]-[0164], pg. 7, lines 43-53). A first message including the calculated first value is sent from the first device to the second device to confirm ownership of the generated address by the first device. (e.g. paras. [0162]-[0164], pg. 7, lines 43-53).

Claim 38 depends from Claim 36 and further comprises repeating the receiving of the request to confirm ownership, the identification of the number of confirmations previously performed between the first device and the second device, the calculation of the first value, and the sending of the first message including the calculated first value. (e.g. para. [0162], pg. 7, lines 43-47).

Claim 39 depends from Claim 38 and further recites that the first message further includes the identified number of confirmations performed. (e.g. para. [0162], pg. 7, line 47).

Claim 40 depends from Claim 36 and further comprises comparing the identified number of confirmations performed with the identified number of identifications allowed, and based on an outcome of the comparison, identifying a second secret value at the first device. (e.g. para. [0158], pg. 7, lines 33-35).

Claim 42 is directed to a computer-readable medium including computer-readable instructions stored therein that cause the processor to calculate information that confirms ownership of an address by a first device to a second device. (e.g. paras. [0156]-[0165], pg. 7, lines 21-2). Upon execution by the processor, the computer-readable instructions cause the communication device to perform the operations of Claim 29. A number of identifications allowed is identified. (e.g. para. [0158], pg. 7, lines 33-35). A secret value is identified at a first device, wherein the number of identifications allowed is based on a maximum number of times the secret value may be used before the secret value is changed. (e.g. paras. [0157]-[0158], pg. 7, lines 27-35). A first address value is

calculated based on the identified secret value and the identified number of identifications allowed. (e.g. para. [0159], pg. 7, lines 36-42). An address is generated as a concatenation of a second address value and the calculated first address value. (e.g. para. [0159], pg. 7, lines 36-42). The generated address is sent from the first device to a second device. (e.g. para. [0051], pg. 3, lines 7-10; para. [0068], pg. 4, lines 11-14). A request to confirm ownership of the generated address is received from the second device at the first device. (e.g. para. [0069], pg. 4, lines 24-25). A number of confirmations previously performed between the first device and the second device is identified. (e.g. para. [0162], pg. 7, lines 43-47). A first value is calculated based on the identified secret value and the identified number of confirmations performed. (e.g. paras. [0162]-[0164], pg. 7, lines 43-53). A first message including the calculated first value is sent from the first device to the second device to confirm ownership of the generated address by the first device. (e.g. paras. [0162]-[0164], pg. 7, lines 43-53).

Claim 44 depends from Claim 42 and further comprises repeating the receiving of the request to confirm ownership, the identification of the number of confirmations previously performed between the first device and the second device, the calculation of the first value, and the sending of the first message including the calculated first value. (e.g. para. [0162], pg. 7, lines 43-47).

Claim 45 depends from Claim 44 and further recites that the first message further includes the identified number of confirmations performed. (e.g. para. [0162], pg. 7, line 47).

Claim 46 depends from Claim 42 and further comprises comparing the identified number of confirmations performed with the identified number of identifications allowed, and based on an outcome of the comparison, identifying a second secret value at the first device. (e.g. para. [0158], pg. 7, lines 33-35).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

One ground of rejection is presented for review in this appeal: The rejection of Claims 29-47 were rejected under 35 U.S.C. § 103 as being unpatentable over an article titled *Statistically Unique and Cryptographically Verifiable (SUCV) Identifiers and Addresses* by Montenegro *et al.* (Montenegro) in view of U.S. Patent No. 6,067,621 to Yu *et al.* (Yu).

ARGUMENT

I. LEGAL STANDARDS UNDER 35 U.S.C. 103(a)

35 U.S.C. 103(a) states:

> A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Obviousness under 35 U.S.C. 103(a) involves four factual inquiries: (1) the scope and content of the prior art; (2) the differences between the claims and the prior art; (3) the level of ordinary skill in the pertinent art; and (4) secondary considerations, if any, of nonobviousness. *See Graham v. John Deere Co.*, 383 U.S. 1 (1966).

In proceedings before the Patent and Trademark Office, the Examiner bears the burden of establishing a prima facie case of obviousness based upon the prior art. *In re Piasecki*, 745 F.2d 1468, 1471-72 (Fed. Cir. 1984).

According to M.P.E.P. § 706.02(j),

> 35 U.S.C. 103 authorizes a rejection where, to meet the claim, it is necessary to modify a single reference or to combine it with one or more other references. After indicating that the rejection is under 35 U.S.C. 103, the examiner should set forth in the Office action:

(A) the relevant teachings of the prior art relied upon, preferably with reference to the relevant column or page number(s) and line number(s) where appropriate,

(B) the difference or differences in the claim over the applied reference(s),

(C) the proposed modification of the applied reference(s) necessary to arrive at the claimed subject matter, and

(D) an explanation >as to< why >the claimed invention would have been obvious to< one of ordinary skill in the art at the time the invention was made**.

** "To support the conclusion that the claimed invention is directed to obvious subject matter, either the references must expressly or impliedly suggest the claimed invention or the examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the references." *Ex parte Clapp*, 227 USPQ 972, 973 (Bd. Pat. App. & Inter. 1985).

II. REJECTION OF CLAIMS 29-47 UNDER 35 U.S.C. 103(a)

In section 4 of the Final Office Action, Claims 29-47 were rejected under 35 U.S.C. § 103 as being unpatentable over an article titled *Statistically Unique and Cryptographically Verifiable (SUCV) Identifiers and Addresses* by Montenegro *et al.* (Montenegro) in view of U.S. Patent No. 6,067,621 to Yu *et al.* (Yu). For the reasons given below, Appellant submits that the Examiner's rejection of Claims 29-47 is improper and should be reversed.

A. Claims 29, 30, 35, 36, 37, 41-43, and 47

Independent Claim 29 recites in part:

(a) identifying a number of identifications allowed;

(b) identifying a secret value at a first device, wherein the number of identifications allowed is based on a maximum number of times the secret value may be used before the secret value is changed;

(c) calculating a first address value based on the identified secret value and the identified number of identifications allowed;

...

(g) identifying a number of confirmations previously performed between the first device and the second device;

(h) calculating a first value based on the identified secret value and the identified number of confirmations performed; and

Independent Claims 36 and 42 recite similar features.

1. identifying a number of identifications allowed

On page 4 of the Final Office Action, the Examiner states that "Yu discloses identifying a number of identification allowed (see, Fig. 6, Step 660, Counter Value N)." Appellant respectfully disagrees. Yu describes a "user authentication system for authenticating a user using an IC card." (Abstract). Therefore, Yu is not related to confirmations between devices, and thus, numbers of identifications, but instead to authenticating a user using a one time password.

At Col. 5, lines 14-30, Yu states:

> When the terminal and the server further comprise each counter for synchronizing the terminal with the server, the one-time password is determined based upon the random number and the counter value stored in the terminal. The one-time password is generated by the steps of inserting the counter value into a password bit stream produced by performing a one way hash function on the value output through the symmetrical key cipher algorithm, and converting the password bit stream into which the counter value is inserted into a predetermined format. The one-time password generated from the terminal is then received for verification by the steps of extracting a counter value from the received one-time password, comparing the counter value extracted with the counter value of the server, and making the counter values of the counter equal and changing the random number into a random number corresponding to the counter value, when the counter values are not the same.

(Underlining added). At Col. 7, lines 22-28, Yu further states:

> The counter memory 127 stores a counter value for synchronizing the terminal 120 with the server 140. The counter changer 128 changes the counter value into a

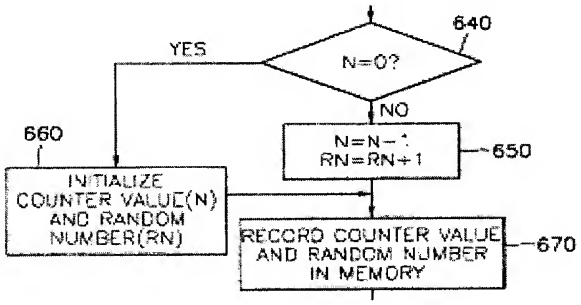
> predetermined value whenever a one-time password is generated, and stores the value in the counter memory 127.

(Underlining added). At Col. 10, lines 43-61, Yu still further states:

> The counter value N is reduced by one each time a password is generated at step 650. The terminal 120 then determines whether the reduced value is 0 at step 640. When the value becomes 0, the process returns to an initial stage. The random number is usually increased by one and initialized when N becomes 0. In the process of initializing the service, the random number read from the IC card 100 is **used only for generating the initial password** and, **after the initial one, the random number is increased by one when each password is generated** at step 650. When the counter value N becomes 0, a random number generated during the generation of the password (for example, the resultant value of the symmetrical key cipher algorithm) is set **as the random number initialized value**. The password is generated by increasing the random number by one at step 650. A new random number is set when the counter value N becomes 0 at step 660. After generating a password, the counter value N and the random number RN are recorded in the random number memory 122 at step 670.

(Underlining and bolding added).

Thus, the counter value N is used to synchronize the server with the terminal. As clearly also indicated in Fig. 6 of Yu reproduced below, if the counter value is not zero, the counter is decremented and the random number is incremented; whereas if the counter value is zero, the counter and the random number are both reset to initial values.



Therefore, as the counter value N is used to indicate when the random number should be reset to an initial value after being repeatedly incremented, it cannot be said to be "a number of identifications allowed" because there is no association between a

number of identifications and the resetting of the random number which is reset each time in any case. As a result, Yu fails to disclose, teach, or suggest "identifying a number of identifications allowed" as recited in Claim 29, and similarly recited in Claims 36, and 42.

2. wherein the number of identifications allowed is based on a maximum number of times the secret value may be used before the secret value is changed

On page 4 of the Final Office Action, the Examiner states that "Yu discloses ... wherein the number of identifications allowed is based on a maximum number of times the secret value may be used before the secret value is changed (see, Fig. 6, Numerals 640 and 660 and also see, Column 10, lines 43-61, system uses a new random number when N reaches zero)." Appellant respectfully disagrees. At Col. 10, lines 43-61 cited by the Examiner, Yu states:

> The counter value N is reduced by one each time a password is generated at step 650. The terminal 120 then determines whether the reduced value is 0 at step 640. When the value becomes 0, the process returns to an initial stage. The random number is usually increased by one and initialized when N becomes 0. In the process of initializing the service, the random number read from the IC card 100 is **used only for generating the initial password** and, **after the initial one, the random number is increased by one when each password is generated** at step 650. When the counter value N becomes 0, a random number generated during the generation of the password (for example, the resultant value of the symmetrical key cipher algorithm) is **set as the random number initialized value**. The password is generated by increasing the random number by one at step 650. A new random number is set when the counter value N becomes 0 at step 660. After generating a password, the counter value N and the random number RN are recorded in the random number memory 122 at step 670.

(Underlining and bolding added).

As discussed above, if the counter value is not zero, the counter is decremented and the random number is incremented; whereas if the counter value is zero, the counter and the random number are both reset to initial values. Therefore, the counter is used to indicate when the random number should be reset to an initial value after being

repeatedly incremented. Thus, the counter value as taught by Yu is not "based on a maximum number of times the secret value may be used before the secret value is changed" as recited in Claim 29, and similarly recited in Claims 36, and 42.

First, nowhere does Yu disclose, teach, or even suggest changing the secret key. Second, the random number is reset for each increment of the counter and is reset to an initial value when the counter goes to zero. Thus, the secret key is not changed, and the random number is changed each time a password is created. As a result, the counter value N, as taught by Yu, is used to synchronize the server and the terminal and is not, in any way, associated with "a maximum number of times the secret value may be used before the secret value is changed" as recited in Claim 29, and similarly recited in Claims 36, and 42. As a result, Yu fails to provide any such teaching.

3. calculating a first address value based on the identified secret value and the identified number of identifications allowed

On page 3 of the Final Office Action, the Examiner states that "Montenegro discloses ... calculating a first address value based on the identified secret value (Section 5.3)." The Examiner ignores the remaining portion of the claim, that is the claim element "the identified number of identifications allowed," thus recognizing that Montenegro fails to provide any suggestion or teaching related to "the identified number of identifications allowed."

As discussed in Sections II.A.1. and II.A.2., Yu also fails to disclose, teach, or suggest "identifying a number of identifications allowed." Therefore, neither Montenegro nor Yu disclose, teach, or suggest "calculating a first address value based on the identified secret value and the identified number of identifications allowed" (underlining added) as recited in Claim 29, and similarly recited in Claims 36, and 42.

4. identifying a number of confirmations previously performed between the first device and the second device

On page 4 of the Final Office Action, the Examiner states that "Yu discloses ... identifying a number of confirmations previously performed between the first device and the second device (see Fig. 7, and also see, Column 10, lines 63-67)." Appellant respectfully disagrees. At column 10, lines 63-67 cited by the Examiner, Yu states:

> FIG. 7 illustrates a process for verifying the one-time password transferred by the user from the portable terminal 120 to the server 140 of the service provider. The server 140 receives the one-time password transferred by the user through the password receiver 142 at step 700.

Thus, the recited section of Yu fails to recite anything whatsoever related to "identifying a number of confirmations previously performed between the first device and the second device" as recited in Claim 29, and similarly recited in Claims 36, and 42. As stated previously, Yu describes a "user authentication system for authenticating a user using an IC card." (Abstract). Therefore, Yu is not related to confirmations between devices, but instead to authenticating a user using a one time password. Therefore, Yu fails to disclose, teach, or suggest "identifying a number of confirmations previously performed between the first device and the second device" as recited in Claim 29, and similarly recited in Claims 36, and 42. The Examiner further recognizes that Montenegro fails to provide any such teaching.

5. calculating a first value based on the identified secret value and the identified number of confirmations performed

On page 3 of the Final Office Action, the Examiner states that "Montenegro discloses ... calculating a first value based on the identified secret value and the identified number of confirmations performed (section 6.2)." Appellant respectfully disagrees. At section 6.2 cited by the Examiner, Montenegro states:

> A sucvP3 message contains the following fields: *Puzzle reply, Public key and imprint* it has used to generate its HID, a *Diffie-Hellman value, the skey_espauth lifetime* and an *SPI* for the CN to use when sending BA's (secured via ESP) to the MN. This message must be signed by the MN with its private key (the public key is used to generate the HID).

The recited section of Montenegro fails to recite anything whatsoever related to "calculating a first value based on the identified secret value and the identified number of confirmations performed" as recited in Claim 29, and similarly recited in Claims 36, and 42. Therefore, Montenegro fails to disclose, teach, or suggest "calculating a first value based on the identified secret value and the identified number of confirmations performed" as recited in Claim 29, and similarly recited in Claims 36, and 42.

Thus, Montenegro and Yu, alone and in combination, fail to disclose, teach, or suggest a number of the elements of at least independent Claims 29, 36, and 42. A rejection under 35 U.S.C. 103(a) cannot be properly maintained where the references used in the rejection do not disclose all of the recited claim elements. Claims 30, 35, 37, 41, and 43, depend from one of Claims 29, 36, and 42. Therefore, Appellant respectfully requests withdrawal of the rejection of Claims 29, 30, 35, 36, 37, 41-43, and 47.

B. Claims 31, 38, and 44

Claim 31 recites:

> The method of claim 29, further comprising repeating (f), (g), (h), (i)

Claims 38 and 44 recite a similar feature.

On pages 4-5 of the Final Office Action, the Examiner states that "[r]egarding Claims 31, 38 and 44, the combination of Montenegro and Yu further discloses repeating (f), (g), (h), (i) (see, Montenegro, last paragraph section 6.2)." Appellant respectfully disagrees.

At section 6.2 cited by the Examiner, Montenegro states:

> As long as the MN uses the same HID interface identifier for its CoA, it does not have to prove the CoA ownership and BU authentication is enough.

> Proving the CoA ownership can be very useful to prevent a malicious host from bombing a victim with packets by using the victim's address as CoA. For example, with "regular" Mobile IPv6, a host can start a big file transfer from a server and then send a BU with the victim's address as CoA to the server. As a result, the file will be send to the victim. If an host can prove that it owns its CoA, and that therefore it is not using someone's else address as CoA, this attack can be avoided.
>
> If for any reason the MN configures its CoA with a new interface identifier, it must restart the whole protocol sequence.

(Underlining added).

The recited section of Montenegro fails to recite anything whatsoever related to repeating the receiving of the request to confirm ownership, the identification of the number of confirmations previously performed between the first device and the second device, the calculation of the first value, and the sending of the first message including the calculated first value as recited in Claim 29, and similarly recited in Claims 36, and 42.

Therefore, Montenegro and Yu fail to disclose, teach, or suggest "repeating (f), (g), (h), (i)" as recited in Claim 31, and similarly recited in Claims 38 and 44. A rejection under 35 U.S.C. 103(a) cannot be properly maintained where the references used in the rejection do not disclose all of the recited claim elements. Therefore, Appellant respectfully request withdrawal of the rejection of Claims 31, 38, and 44.

C. Claims 32, 39, and 45

Claim 32 recites:

> The method of claim 31, wherein the first message further includes the identified number of confirmations performed

Claims 39 and 45 recite a similar feature.

On page 5 of the Final Office Action, the Examiner states that "[r]egarding Claims 32, 39 and 45, the combination of Montenegro and Yu further discloses wherein the first message further includes the identified number of confirmation performed (see, Yu, Fig. 7, Numerals 700 and 710)." Appellant respectfully disagrees. Yu states:

> FIG. 7 illustrates a process for verifying the one-time password transferred by the user from the portable terminal 120 to the server 140 of the service provider. The server 140 receives the one-time password transferred by the user through the password receiver 142 at step 700. Then, the server 140 extracts the counter value from the data bit stream received by the counter extractor 148 at step 710 and synchronizes with the terminal 120. The server 140 generates a one-time password by the same method as in the terminal, using the synchronized random number and secret number at step 720. Since the process for generating the one-time password is the same as that in the terminal, an explanation thereof is omitted. Then, the one-time password generated from the server 140 is compared with the one-time password generated by the user from the portable terminal 120 at step 730. If the two passwords are identical, the identity of the user is authenticated at step 770.

(Underlining added).

As discussed in Sections II.A.1.-5., the counter value as taught by Yu is not related to a "number of confirmations performed," and Yu fails to disclose, teach, or suggest "wherein the first message further includes the identified number of confirmations performed" as recited in Claim 32, and similarly recited in Claims 39, and 45. Yu simply fails to provide any such teaching. The Examiner further recognizes that Montenegro fails to provide any such teaching. A rejection under 35 U.S.C. 103(a) cannot be properly maintained where the references used in the rejection do not disclose all of the recited claim elements. Therefore, Appellant respectfully requests withdrawal of the rejection of Claims 32, 39, and 45.

D. Claims 33, 40, and 46

Claim 33 recites:

> The method of claim 29, further comprising:
>
> (j) comparing the identified number of confirmations performed with the identified number of identifications allowed; and
>
> (k) based on an outcome of the comparison, identifying a second secret value at the first device.

Claims 40 and 46 recite a similar feature.

On page 5 of the Final Office Action, the Examiner states:

> Regarding Claim 33, 40 and 46, the combination of Montenegro and Yu further discloses comparing the identified number of confirmations performed with the identified number of identification allowed; and based on outcome of the comparison, identifying a second secret value at the first device (see, Yu, Column 10, lines 43-61, system uses a new random number when N reaches zero).

At Col. 10, lines 43-61 cited by the Examiner, Yu states:

> The counter value N is reduced by one each time a password is generated at step 650. The terminal 120 then determines whether the reduced value is 0 at step 640. When the value becomes 0, the process returns to an initial stage. The random number is usually increased by one and initialized when N becomes 0. In the process of initializing the service, the random number read from the IC card 100 is **used only for generating the initial password** and, **after the initial one, the random number is increased by one when each password is generated** at step 650. When the counter value N becomes 0, a random number generated during the generation of the password (for example, the resultant value of the symmetrical key cipher algorithm) is set as the random number initialized value. The password is generated by increasing the random number by one at step 650. A new random number is set when the counter value N becomes 0 at step 660. After generating a password, the counter value N and the random number RN are recorded in the random number memory 122 at step 670.

(Underlining and bolding added).

As discussed Sections II.A.1.-5., the counter value as taught by Yu is not related to a "number of confirmations performed," and Yu fails to disclose, teach, or suggest "comparing the identified number of confirmations performed with the identified number of identifications allowed" as recited in Claim 33, and similarly recited in Claims 40, and 46.

Yu further fails to provide any teaching related to "based on an outcome of the comparison, identifying a second secret value at the first device" as recited in Claim 33, and similarly recited in Claims 40, and 46. First, nowhere does Yu disclose, teach, or suggest changing the secret key. Thus, a second secret value is never identified

irrespective of the counter value N. Second, the random number is reset for each increment of the counter, and is reset to an initial value when the counter goes to zero. Thus, the secret key is not changed, and the random number is changed each time a password is created. As a result, the Examiner's statement that "system uses a new random number when N reaches zero" (page 5 of the Final Office Action) mischaracterizes the reference. The system uses a new random number each time until N reaches zero when the random number is reset to an initial value which is not new. As a result, Yu fails to provide any such teaching. The Examiner further recognizes that Montenegro fails to provide any such teaching. A rejection under 35 U.S.C. 103(a) cannot be properly maintained where the references used in the rejection do not disclose all of the recited claim elements. Therefore, Appellant respectfully requests withdrawal of the rejection of Claims 33, 40, and 46.

E. Claim 34

Claim 34 recites:

> The method of claim 33, further comprising repeating (c)-(i) replacing the identified secret value with the identified second secret value.

On page 5 of the Final Office Action, the Examiner states:

> Regarding Claim 34, the combination of Montenegro and Yu further discloses repeating (c)-(i) replacing the identified secret value with the identified second secret value (see, Montenegro, section 6.4 and Vu, Fig. 6).

At section 6.4 cited by the Examiner, Montenegro states:

> The following algorithms must be supported by any SUCV implementation:
>
> • DSA [5] for signing sucvP3.
>
> • Diffie-Hellman Oakley Group 1 [25] for the ephemeral Diffie-Hellman exchange.
>
> • HMAC-SHA-I-96 (24] for ESP authentication.
>
> • 3DES-CBC [26] for sucvP5 and ESP encryption.

The recited section of Montenegro fails to recite anything whatsoever related to repeating the calculation of the first address value, the generation of the address, the sending of the generated address, the receiving of the request to confirm ownership, the identification of the number of confirmations previously performed between the first device and the second device, the calculation of the first value, and the sending of the first message including the calculated first value as recited in Claim 34.

Yu further fails to provide any teaching related to "identifying a second secret value at the first device" as discussed in Section II.D. Thus, Yu cannot provide any teaching related to "repeating (c)-(i) replacing the identified secret value with the identified second secret value" as recited in Claim 34. Therefore, Montenegro and Yu fail to disclose, teach, or suggest "repeating (c)-(i) replacing the identified secret value with the identified second secret value" as recited in Claim 34. A rejection under 35 U.S.C. 103(a) cannot be properly maintained where the references used in the rejection do not disclose all of the recited claim elements. Therefore, Appellant respectfully requests withdrawal of the rejection of Claims 34.

CONCLUSION

In view of the foregoing discussion and arguments, Appellant respectfully submits that Claims 29-47 are not properly rejected under 35 U.S.C. § 103(a) as being unpatentable over Montenegro in view of Yu. Accordingly, Appellant respectfully requests that the Board reverse all claim rejections and indicate that a Notice of Allowance respecting all pending claims should be issued.

Respectfully submitted,

Date December 8, 2008

By _____

FOLEY & LARDNER LLP
Customer Number: 23524
Telephone: (608) 258-4263
Facsimile: (608) 258-4258

Callie M. Bell
Attorney for Appellant
Registration No. 54,989

CLAIMS APPENDIX

1. - 28. (Canceled)

29. (Previously presented) A method of confirming ownership of an address by a first device to a second device, the method comprising:

(a) identifying a number of identifications allowed;

(b) identifying a secret value at a first device, wherein the number of identifications allowed is based on a maximum number of times the secret value may be used before the secret value is changed;

(c) calculating a first address value based on the identified secret value and the identified number of identifications allowed;

(d) generating an address as a concatenation of a second address value and the calculated first address value;

(e) sending the generated address from the first device to a second device;

(f) receiving a request to confirm ownership of the generated address from the second device at the first device;

(g) identifying a number of confirmations previously performed between the first device and the second device;

(h) calculating a first value based on the identified secret value and the identified number of confirmations performed; and

(i) sending a first message from the first device to the second device, the first message including the calculated first value so that the second device can confirm ownership of the generated address by the first device.

30. (Previously Presented) The method of claim 29, further comprising receiving a router advertisement message including an address prefix, wherein the second address value comprises the address prefix.

31. (Previously Presented) The method of claim 29, further comprising repeating (f), (g), (h), (i).

32. (Previously Presented) The method of claim 31, wherein the first message further includes the identified number of confirmations performed.

33. (Previously Presented) The method of claim 29, further comprising:

(j) comparing the identified number of confirmations performed with the ~~defined~~ identified number of identifications allowed; and

(k) based on an outcome of the comparison, identifying a second secret value at the first device.

34. (Previously Presented) The method of claim 33, further comprising repeating (c)-(i) replacing the identified secret value with the identified second secret value.

35. (Previously Presented) The method of claim 29, wherein the first message comprises a binding update message sent using a mobile Internet protocol version 6 protocol.

36. (Previously Presented) A communication device, the communication device comprising:

a processor;

a communication interface operably coupled to the processor; and

a computer-readable medium including computer-readable instructions stored therein that, upon execution by the processor, perform operations comprising

(a) identifying a number of identifications allowed;

(b) identifying a secret value, wherein the number of identifications allowed is based on a maximum number of times the secret value may be used before the secret value is changed;

(c) calculating a first address value based on the identified secret value and the identified number of identifications allowed;

(d) generating an address as a concatenation of a second address value and the calculated first address value;

(e) sending the generated address to a second device via the communication interface;

(f) receiving a request to confirm ownership of the generated address from the second device via the communication interface;

(g) identifying a number of confirmations previously performed between the communication device and the second device;

(h) calculating a first value based on the identified secret value and the identified number of confirmations performed; and

(i) sending a first message to the second device via the communication interface, the first message including the calculated first value so that the second device can confirm ownership of the generated address.

37. (Previously Presented) The communication device of claim 36, wherein the operations further comprise receiving a router advertisement message including an address prefix, wherein the second address value comprises the address prefix.

38. (Previously Presented) The communication device of claim 36, wherein the operations further comprise repeating (f), (g), (h), (i).

39. (Previously Presented) The communication device of claim 38, wherein the first message further includes the identified number of confirmations performed.

40. (Previously Presented) The communication device of claim 36, wherein the operations further comprise:

(j) comparing the identified number of confirmations performed with the defined number of identifications allowed; and

(k) based on an outcome of the comparison, identifying a second secret value at the communication device.

41. (Previously Presented) The communication device of claim 36, wherein the first message comprises a binding update message sent using a mobile Internet protocol version 6 protocol.

42. (Previously Presented) A computer-readable medium including computer-readable instructions that, upon execution by a processor, cause the processor to calculate information that confirms ownership of an address by a first device to a second device, the instructions configured to cause a computing device to:

(a) identify a number of identifications allowed;

(b) identify a secret value, wherein the number of identifications allowed is based on a maximum number of times the secret value may be used before the secret value is changed;

(c) calculate a first address value based on the identified secret value and the identified number of identifications allowed;

(d) generate an address as a concatenation of a second address value and the calculated first address value;

(e) send the generated address to a second device;

(f) receive a request to confirm ownership of the generated address from the second device;

(g) identify a number of confirmations previously performed between a first device and the second device;

(h) calculate a first value based on the identified secret value and the identified number of confirmations performed; and

(i) send a first message to the second device, the first message including the calculated first value so that the second device can confirm ownership of the generated address.

43. (Previously Presented) The computer-readable medium of claim 42, wherein the instructions are further configured to cause the computing device to receive a router advertisement message including an address prefix, wherein the second address value comprises the address prefix.

44. (Previously Presented) The computer-readable medium of claim 42, wherein the instructions are further configured to cause the computing device to repeat (f), (g), (h), (i).

45. (Previously Presented) The computer-readable medium of claim 44, wherein the first message further includes the identified number of confirmations performed.

46. (Previously Presented) The computer-readable medium of claim 42, wherein the instructions are further configured to cause the computing device to:

(j) compare the identified number of confirmations performed with the identified number of identifications allowed; and

(k) based on an outcome of the comparison, identify a second secret value.

47. (Previously Presented) The computer-readable medium of claim 42, wherein the first message comprises a binding update message sent using a mobile Internet protocol version 6 protocol.

48. -89. (Cancelled)

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.